SECRET

25X1

DIRECTOR OF CENTRAL INTELLIGENCE
Intelligence Information Handling Committee
WASHINGTON, DC 20505

[redacted]

LOGGED

[redacted]

ICS 4236-88
15 June 1988

25X1

MEMORANDUM FOR: See Distribution

SUBJECT: Definition of a Multilateral Counterterrorist Data System (MCDS)

REFERENCE: DDCI Memorandum, Subj: Development of the Multilateral Counterterrorist Data System (MCDS), Dated 16 November 1987

1. Attachment A, for your review, is the draft Terms of Reference (TOR) of a fast-track, exploratory initiative to define an MCDS that will achieve the objectives set forth by the Deputy Director of Central Intelligence in referenced memorandum to NFIB Principals. The effort will use, as its point of departure, the conceptual outline (Attachment B) circulated earlier in the counterterrorism community by the IHC. It will address (a) the technical and operational implications of implementing the concept or a variant considered more promising; (b) the projected cost of doing so; and (c) policy and procedural aspects of agency participation in MCDS development and operation. Findings will be reflected in a report to the DDCI in which a follow-on course of action will be recommended.

2. CIA, DIA, NSA, and DOS should be represented in all working groups indicated in the TOR. Other counterterrorism community members may be represented selectively as they choose. All agencies should participate in the Concept of Operations Working Group. Major working papers and the final report draft will be provided to all community members for review.

3. A general meeting of working group members will be held at 1000 on 29 June 1988 [redacted] 25X1
[redacted] Please advise [redacted] 25X11
of your assignees to the various working groups. The meeting will review the TOR and address procedural matters attendant to the study.

[redacted] 25X1

Attachments:
As stated

[redacted] 25X1

SECRET

SUBJECT: Definition of a Multilateral Counterterrorist Data System (MCDS)

Distribution: ICS 4236-88
1 - USA/Hqs DA/DAMI-CIC (LtCol J. Lewin)
1 - USAF/INXD (Capt. Koloian)
1 - USAF/OSI (G. Mayo)
1 - USN/NSIC (W. Vonstorch)
1 - USN/DNI/OP-92P (Maj. N. Taylor)
1 - DIA [redacted] 25X1
1 - DOE (LtCol D. Jernigan, USA)
1 - STATE/INR/TNA (J. Arriza)
1 - NSA/G1 [redacted] 25X1
1 - CIA [redacted] 25X1
1 - CIA Comptroller
1 - D/CTC/CIA
1 - D/OIT/CIA
1 - Ea. Member, IICT
1 - Ea. Member, IHC
1 - IHC Subj
1 - IHC Chrono
1 - ICS Reg

Next 1 Page(s) In Document Denied

Attachment B

MCDS: Concept of Design and Operations

Principal Operational Objective

To facilitate counterterrorist operations and intelligence analysis by providing improved communications, information handling and data base access in a secure operating environment.

Basic System Design Concept

MCDS would be designed to function as a community-specific system, meaning that it would be technically and functionally structured to support a limited, pre-defined body of users, i.e., the counterterrorism community. This approach would permit adoption of technical and procedural security controls needed to maximize protection of intelligence sources and methods while facilitating a relatively uninhibited interchange of information within the community the system supports. It would also aid in tailoring system capacities and capabilities to maximize responsiveness.

MCDS would be a closed system without interactive connection to any other system. Data could be entered into the system online, but could not be transferred out of the system electronically. Outputs would be limited to system controlled peripherals (display terminals, printers, etc) that could not further transfer the data without human intervention. Additional security features would include:

- o centrally monitored terminal access control (personal identification verification)
- o automatic collection of audit trail data: user activity, internal data transfers, outputs, interstation communications, etc.
- o automated monitoring of audit data (intrusion detection expert system)
- o superencryption of data transmitted via multiuser networks, e.g. DODIIS.
- o operate as a compartmented mode system per DCID 1/16.

Operationally, MCDS would view its subscribers as members of the defined counterterrorism community rather than of a spectrum of separate agencies and commands. Dissemination of reports and access to data bases within MCDS would, therefore, be determined on a functional rather than organizational basis. An authorized MCDS subscriber would have access to all data within the system that corresponded to an established need-to-know profile reflecting the scope of his or her assigned counterterrorism operations or analysis duties.

25X1

Task Objective

To define a projected Multilateral Counter Terrorist Data System (MCDS) to a level of specificity and with sufficient detail to:

- provide senior Community management, a description of projected system capabilities and concept of operations necessary to support an implementation decision;

- serve as the basis of a contingent agreement among participating organizations to support development and operation of the MCDS as defined;

- assure that the proposed concept of operations and associated capabilities are functionally and technically achievable at an acceptable level of cost and risk;

- establish the basis for technical and functional system security design acceptable to Community accrediting authorities;

- support reliable estimation of the cost to build and operate the system; and

- serve as the point of departure for a system development program, following a DCI/DDCI decision to implement.

Task Execution Methodology

Definition of the MCDS will be based on: (1) the concept of operations outlined by the Intelligence Information Handling Committee (attached) and reviewed by the Interagency Committee on Counterterrorism, and (2) the MCDS Follow-On Study Report of 25 March 1988 (to be provided separately) prepared under the auspices of the CIA Counterterrorism Center. The projected system will supplant the current Decision Support and Information System for Terrorism (DESIST) and FLASHBOARD as either a lineal improvement or a substantial replacement, the determination to reflect, inter alia, the findings of this system definition effort. Commensurate with MCDS operating and security requirements, as much of the current DESIST information handling system as possible should be utilized. Its associated International Terrorist Profile and CENTIPEDE data bases will, in any event, be continued in MCDS, regardless of its configuration.

The MCDS definition will be developed in three segments, the first to address functional and performance requirements, the second to explore the system design and capabilities implications of those requirements, and the third to assess the cost of implementation and operation. While it is logical to address the segments consecutively, aspects of all three will need to be considered in parallel if the effort is to result in a pragmatic development program. A follow-on fourth segment will seek to structure a multi-year implementation strategy based on the findings of segments two and three.

To facilitate rapid development of the MCDS system definition, its major components, will be addressed separately, but simultaneously, by working groups comprised of appropriate personnel from participating agencies. The working groups will have technical and administrative contractor support. They will identify first the functional and performance requirements within their respective components and then their system design implications in terms of information handling capabilities and capacities. The latter will then be integrated to form a composite system description. The IHC Staff will coordinate the overall effort to insure necessary interaction among the working groups and completeness of the integrated product.

Upon completion of the system description, the technical support contractor will prepare an estimate of system implementation costs, taking into account, as appropriate, the prospective use of existing assets and capabilities, such as DESIST, FLASHBOARD, DoDIIS, etc. Finally, a phased implementation strategy seeking to achieve an initial operating capability as rapidly as possible, commensurate with available funding, will be prepared. All of the foregoing will be coordinated with participating Community organizations prior to submission to the DCI/DDCI.

Level of Detail

The key to the foregoing methodology is the specificity and detail to which the MCDS system definition is developed. Too little will preclude useful estimation of system development and operating costs; too much will bog down the working groups and obscure the functional and economic questions most relevant to senior management.

The system definition should be limited to establishing significant functional requirements and their technical design implications, the latter being necessary to implementation cost estimation. No extensive detail regarding how the requirements are to be met will be documented; however, the working groups, in translating requirements into the system definition, will include only those which are technically and operationally achievable, as well as cost effective. Technical design implications will be elaborated only to the extent needed to derive cost estimations. An example of the foregoing is the functional requirement that MCDS subscribers be able to informally communicate with one another through the system. Provision of this capability, in turn, implies a system architecture featuring a central processing or switching facility through which all terminals are interconnected. A related requirement that a record be made of such communications for security auditing purposes yields additional implications regarding configuration of the central facility, etc.

Working Group Organization

The following is the proposed working group structure and major system elements that should be addressed by each. The working groups will operate simultaneously, with the system architecture group lagging, insofar as its findings must reflect the output of the other groups.

System Architecture and Communications Working Group

- Central processor specifications and capacities
- Operating system
- Data base management system
- Intermediate processors, switches etc.
- System redundancy/survivability
- Access terminal specifications
- Central processor-terminal connectivity
- Common user network utilization
- Transmission capacity requirements (photos, graphics, etc.)
- Message traffic direct input

Security Working Group

- Access control
- Auditing
- User profiling
- Internal compartmentation
- Physical security requirements
- Electronic security requirements
- Network Security Requirements

User Services Working Group

- User terminal facilities
- Query and retrieval; data integration
- Report generation
- Interstation communications
- Graphics
- Analytical aids
- Alerts
- Message traffic dissemination
- Retrospective query and retrieval
- System databases and maintenance procedures
- Data handling and storage capacities

Concept of Operations Working Group

(See below)

Concept of Operations Definition

In parallel with the system definition effort outlined above, the concept of MCDS operations must be developed to the level of specificity needed to serve as the basis of a formal Community understanding concerning MCDS operations, support responsibilities, and security. MCDS design will be substantially influenced by the dual goals of providing less inhibited intelligence support to counterterrorist operations and analysis while adequately safeguarding the intelligence sources and methods involved. Achieving them will require functional, procedural, and technical trade-offs in system configuration and operation that will, in turn, reflect policy and management decisions by the Community agencies sponsoring MCDS. Those decisions will be a prerequisite to MCDS implementation.

The Concept of Operations Working Group will serve as the medium for development of the above. It will comprise representatives of the agencies principally affected by MCDS requirements and operations; however, all agencies participating in MCDS support and utilization will review and contribute to the working group's findings. The formalized understanding reached will be included in the MCDS implementation proposal submitted to the DCI/DDCI.

Questions to be addressed in the MCDS Concept of Operations will include:

- Access terminal deployment
- Access control and monitoring responsibility
- Need-to-know determination and administration
- Dynamic data input contributions
- Reference database contributions and maintenance responsibilities
- Interstation communications policy and procedures
- System security administration
- System configuration control management
- System operational management
- System operating and maintenance cost underwriting